

Informativa sulla sicurezza Home, Mobile e Corporate Banking della Cassa di Risparmio di Volterra SpA

Credenziali previste per Home e Mobile Banking destinati ai clienti “Privati”

Per accedere all'Home e Mobile Banking vengono richiesti due diversi codici:

- il Codice Utente che è quello indicato nel contratto e inviato tramite e-mail all'indirizzo riportato nel contratto stesso;
- la Password scelta dall'Utente dopo l'accesso iniziale (al primo accesso è richiesta la password fornita dalla Banca e ricevuta tramite SMS). La Password non deve essere di semplice intuizione evitando riferimenti personali o familiari. E' inoltre necessario modificare periodicamente la password a tutela dell'Utente nonché per evitare il blocco del dispositivo trascorsi 180 dall'ultima modifica.

Dopo l'accesso iniziale il sistema chiederà di rispondere ad almeno tre domande di sicurezza per permettere, in futuro, in caso di blocco del dispositivo, di poter riattivare il dispositivo in completa autonomia senza necessità di ricorrere al servizio di Assistenza della Banca.

Per impartire disposizioni di pagamento è necessario inserire il codice OTP (One Time Password) generato dal Token Hardware o Software assegnato dalla Banca all'Utente.

L'Utente deve conservare le credenziali ed il Token Hardware o Software con cura, evitando di comunicarli o consegnarli a terzi.

Credenziali previste per Corporate Banking destinati ai clienti “Business”

Per accedere al Corporate Banking vengono richiesti tre diversi codici:

- il Codice Postazione che è quello indicato nel contratto e inviato tramite e-mail all'indirizzo riportato nel contratto stesso;
- il Codice PIN scelto dall'Utente con l'accortezza che non sia un codice di semplice intuizione né contenga riferimenti progressivi od identici;
- la Password scelta dall'Utente dopo l'accesso iniziale (al primo accesso è richiesta la password fornita dalla Banca e ricevuta tramite SMS). La Password non deve essere di semplice intuizione evitando riferimenti personali o familiari. E' inoltre necessario modificare periodicamente la password a tutela dell'Utente nonché per evitare il blocco del dispositivo trascorsi 180 dall'ultima modifica.

Per impartire disposizioni di pagamento o di presentazioni è necessario inserire il codice OTP (One Time Password) generato dal Token Hardware assegnato dalla Banca all'Utente.

L'Utente deve conservare le credenziali ed il Token Hardware con cura, evitando di comunicarlo o consegnarlo a terzi.

Requisiti Hardware e Software del PC dell'Utente

I requisiti minimi per gli applicativi di Home, Mobile e Corporate Banking sono i seguenti:

Home e Corporate Banking

- Hardware: non previsti requisiti minimi
- Software: previsti i seguenti requisiti minimi
 - ✓ MICROSOFT INTERNET EXPLORER versione IE7 e superiori
 - ✓ CHROME versione 5 e superiori
 - ✓ FIREFOX versione 5 e superiori
 - ✓ OPERA versione 11 e superiori
 - ✓ SAFARI versione 4 e superiori

Mobile Banking

- Hardware Smartphone e Tablet: non previsti requisiti minimi
- Software Smartphone e Tablet Software: previsti i seguenti requisiti minimi
 - ✓ APPLE IOS SAFARI MOBILE versione 5 e superiori
 - ✓ ANDROID MOBILE GOOGLE CHROME versione 3 e superiori

Protocollo di sicurezza

Tutti i dati e le informazioni, su PC e App della Banca, sono protetti con il sistema più avanzato di crittografia SSL a 128 bit.

Per entrare nel sito della Banca deve essere sempre:

- verificato che la trasmissione dei dati sia protetta (presenza di un lucchetto chiuso sulla finestra del browser);
- verificato che sia presente il prefisso <https://>
- effettuato l'accesso dal sito istituzionale della Banca www.crvolterra.it evitando l'accesso da link diversi;
- verificato di non aver memorizzato la password sul sistema di navigazione.

Tentativi di accesso

Per la sicurezza e tutela dell'Utente, sono a disposizione tre tentativi consecutivi per la corretta digitazione della password o del PIN (se il tuo applicativo è un Business).

Al terzo tentativo errato l'applicativo viene bloccato dal sistema.

Il blocco del dispositivo può essere resettato dalla Banca o, se trattasi di un Home Banking "Privati", in autonomia dall'Utente tramite le risposte segrete di sicurezza.

Durata della sessione inattiva

Per la sicurezza e tutela dell'Utente, trascorsi 20 minuti di inattività, la connessione con la Banca decade ed apparirà un avviso di sessione scaduta.

Per rientrare deve essere nuovamente eseguito l'accesso.

Procedura di pagamento via Internet

Le disposizioni di pagamento disposte via Internet prevedono un'operatività progressiva:

- *inoltro*: operazione tramite la quale l'Utente predispone ed inserisce via internet - con valorizzazione di tutti i campi obbligatori previsti - una disposizione;
- *salvataggio*: operazione – facoltativa – che permette di salvare la disposizione inserita prima dell'autorizzazione;
- *autorizzazione*: operazione che, tramite digitazione del codice OTP prodotto dal Token Hardware o Software - permette l'autorizzazione della disposizione. Con tale azione la disposizione viene trasferita al sottosistema (conti correnti, deleghe, portafoglio, carte..) che esegue la registrazione sul conto corrente e l'inoltro alla controparte;
- *esito*: la conferma dell'esecuzione della disposizione autorizzata viene comunicata all'Utente tramite e-mail nonché resa visibile sul conto corrente con registrazione contabile variabile a secondo del sottosistema interessato.

Orientamenti per la sicurezza dei dispositivi

Per la sicurezza e tutela dell'Utente e del servizio, l'Utente deve aggiornare costantemente il proprio sistema con programmi Antivirus (per proteggere il dispositivo da virus, malware, spyware, app non sicure e altre minacce) e Firewall (per proteggere il dispositivo da intrusioni indesiderate) per mantenere aggiornata la sicurezza di questi programmi.

Analoga cura deve essere seguita nella custodia dei dispositivi portatili, tablet e smartphone.

Procedura in caso di abuso riscontrato o sospetto

Nel caso di abuso riscontrato o sospetto, per evitare possibili ricadute negative in termini di sicurezza, l'Utente deve:

- eseguire senza indugio il blocco del dispositivo (PC, tablet, smartphone) in autonomia digitando tre volte consecutive in maniera errata la password di accesso o, qualora impossibilitati, comunicare l'evento alla Banca od al soggetto terzo designato per l'esecuzione del blocco
- inviare senza indugio alla Banca segnalazione su (presunti) pagamenti fraudolenti, incidenti sospetti o anomalie durante la sessione per i servizi di pagamento via Internet accedendo al sito istituzionale della Banca alla sezione "Contatti" e compilando il form predisposto sotto la voce "Sicurezza pagamenti via Internet". La Banca, eseguiti i controlli del caso, fornirà risposta all'Utente direttamente nell'applicativo.

Procedura di segnalazioni di sicurezza

I dispositivi hardware e software e le credenziali riservate sono elementi interfunzionali.

Il possibile abuso, perdita o furto necessita da parte dell'Utente di immediate azioni volte a impedire l'utilizzo fraudolento.

- *perdita e furto delle credenziali*: l'Utente deve comunicare senza indugio il furto, lo smarrimento o furto delle credenziali di accesso (Codice Utente o Postazione, Password) e di utilizzo (Token Hardware o Software) alla Banca od al soggetto terzo designato
- *perdita e furto dei dispositivi e tentativi di intrusione*: l'Utente deve comunicare senza indugio il furto, lo smarrimento o l'indebita intrusione dei propri dispositivi (PC, tablet, smartphone, token) a tutela della riservatezza delle informazioni e sicurezza del servizio.

Reclami

L'Utente, per eventuali contestazioni inerenti il rapporto tra Banca e cliente, può presentare reclamo, inviando comunicazione scritta all'Ufficio Reclami della Banca all'indirizzo Cassa di Risparmio di Volterra Spa - Ufficio Reclami - Piazza dei Priori, 16/18 56048 Volterra (PI) - o per via telematica tramite il sito web della Banca www.crvolterra.it, sezione "Reclami".

L'Ufficio Reclami riscontrerà il reclamo così ricevuto, inviando comunicazione scritta al Cliente, entro 30 giorni dalla data di ricezione.

Responsabilità dell'Utente e della Banca

Nell'uso del servizio di pagamento via Internet, l'Utente assume responsabilità:

- in mancanza di rispetto dei termini e delle condizioni contrattuali;
- in mancanza dell'immediata adozione di tutte le misure idonee a garantire la sicurezza del servizio e delle credenziali;
- sulla perdita derivante dall'utilizzo indebito del servizio conseguente al furto o smarrimento delle credenziali di accesso/utilizzo per un importo comunque non superiore complessivamente a 150 euro, salvo il caso in cui abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza delle credenziali di accesso/utilizzo del servizio;
- nella trasmissione dei dati tramite la rete Internet pubblica, per i quali assume piena e totale responsabilità, essendo a conoscenza dei rischi insiti nell'utilizzo dei dispositivi per usufruire del servizio.

Nell'uso del servizio di pagamento via Internet, la Banca assume responsabilità:

- sulla garanzia che i dispositivi personalizzati che consentono l'accesso e l'utilizzo al servizio siano accessibili unicamente all'Utente;
- sul divieto di attivare servizi analoghi al servizio non richiesti dall'Utente, a meno che il servizio e/o le credenziali di accesso debbano essere sostituite;
- sull'assicurazione che l'Utente abbia sempre a sua disposizione strumenti adeguati per effettuare in modo efficace la notifica in caso di furto, smarrimento, appropriazione indebita o uso non autorizzato delle credenziali di accesso/utilizzo del servizio e richiedere lo sblocco del servizio;
- sull'impedimento di qualsiasi uso del servizio dopo che il furto, lo smarrimento, l'appropriazione indebita o l'uso non autorizzato delle credenziali sono stati notificati alla Banca;
- sui rischi derivanti dalla spedizione delle credenziali di accesso;

- sui rischi connessi alla continuità operativa del servizio;
- sui rischi connessi alla sicurezza informatica del servizio.

Difesa dai Rischi

AVVISO E-MAIL OPERAZIONI INTERNET

Il sistema invia automaticamente, per ogni disposizione impartita da Internet, e-mail al riferimento presente nel contratto, in modo tale che l'Utente possa avere immediata evidenza delle operazioni disposte ed autorizzate dal canale.

AVVISO SMS ALL'ACCESSO INTERNET

Può essere richiesto il servizio di notifica tramite SMS per la ricezione di un messaggio per ogni accesso effettuato al servizio di Home e Corporate Banking.

AVVISO SMS PRINCIPALI OPERAZIONI SUL CONTO CORRENTE

Può essere richiesto il servizio di notifica tramite SMS per la ricezione di un messaggio per le principali operazioni transitate sul conto corrente.

COMUNICAZIONI PERIODICA SULL'USO CORRETTO E SICURO DEL SERVIZIO

L'Utente sarà informato dalla Banca tramite avviso nel proprio applicativo internet sulle novità in materia di sicurezza del servizio.

CONTROLLO DELLA SITUAZIONE CONTABILE

E' necessario che l'Utente verifichi spesso – on line o tramite app – i movimenti del conto corrente per accorgersi di eventuali operazioni non conformi.

PROTEZIONE DEI DATI PERSONALI

Sulla rete Internet è meglio essere estremamente diffidenti nel consegnare i propri dati riservati senza essere certi dell'identità di chi li sta chiedendo.

Tentativi di "phishing" e di "social engineering" sono sempre più diffusi.

Il "phishing" è una truffa informatica ideata da malviventi per carpire i dati personali di accesso attraverso false e-mail, apparentemente provenienti dalla banca o da una società emittente carte di credito, composte utilizzando logo, nome e il layout tipico dell'azienda imitata. Nella falsa e-mail, ad esempio a causa di un imprecisato problema al sistema di "home banking", viene spesso richiesto di accedere all'home page del sito della banca tramite un link da cliccare indicato nella e-mail stessa. Se si procede nell'operazione digitando Codice Utente e Password, qualcuno si impossesserà dei dati personali dell'Utente.

Se ricevuta e-mail sospetta come quella appena descritta, non deve essere risposto nè deve essere cliccato sui link presenti nella e-mail. L'e-mail non deve essere aperta ma cestinata subito !

Il "social engineering " è una truffa informatica usata da un malvivente che conosce alcuni elementi personali dell'Utente ma non tutti. Nascondendo la propria identità, carpisce la fiducia dell'interlocutore (tramite e-mail o via telefono) fino a ricavare le informazioni necessarie.

La Banca non richiede mai, direttamente o tramite terzi, informazioni personali o codici di accesso ai servizi di Home, Mobile e Corporate Banking.

Ecco alcune semplici regole per evitare di cadere in questo tipo di truffe:

- diffidare di qualunque e-mail che richieda l'inserimento di dati riservati riguardanti codici di accesso al servizio di Home e Corporate Banking o altre informazioni personali;
- è possibile riconoscere le truffe via e-mail con qualche piccola attenzione; generalmente:
 - non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
 - fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'Utente;
 - non riportano una data di scadenza per l'invio delle informazioni.
- nel caso in cui venga ricevuta e-mail contenente richieste di questo tipo, non deve essere risposto né aperti gli allegati od i file eseguibili. L'e-mail deve essere cestinata subito !
- non deve essere cliccato su link presenti in e-mail sospette dato che i collegamenti potrebbero proseguire su di un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, è bene non fidarsi: è possibile infatti visualizzare nella barra degli indirizzi del browser un indirizzo diverso da quello reale;
- diffidare inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @ o con errori grammaticali;
- inserire i dati riservati esclusivamente in una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella pagina è presente un lucchetto chiuso;
- diffidare del cambio di modalità con la quale viene chiesto l'inserimento dei codici di accesso se non provenienti dal sito istituzionale: tramite pop-up, con dimensioni diverse, in lingua diversa;
- diffidare da e-mail o telefonate non richieste da persone che chiedono informazioni dettagliate o complete. Spesso oltre i codici di accesso vengono chiesti anche tutti i riferimenti anagrafici, personali e comportamentali.